Before the

House Energy and Commerce Committee

"Combating Spyware: H.R. 29 The SPY ACT"

David N. Baker
VP, Law & Public Policy
EarthLink, Inc.

As Prepared For Delivery

January 26, 2005

Mr. Chairman, Ladies and Gentlemen of the Committee, thank you for inviting me here today. I am Dave Baker, Vice President for Law and Public Policy with EarthLink. Headquartered in Atlanta, EarthLink is one of the nation's largest Internet Service Providers (ISPs), serving over 5 million customers nationwide with broadband (DSL, cable and satellite), dial-up, web hosting and wireless Internet services. EarthLink is always striving to improve its customers' online experience. To that end, we appreciate the efforts of this committee to combat the growing problem of spyware.

Spyware: A Growing Threat

We have reached a point in time where spyware has equaled if not surpassed spam as the biggest problem facing Internet users. Spyware compromises consumers' online experience and security. As the Wall Street Journal noted even last year, "Indeed, spyware – small programs that install themselves on computers to serve up advertising, monitor Web surfing and other computer activities, and carry out other orders – is quickly replacing spam as the online annoyance computer users most complain about." "What's That Sneaking Into Your Computer?" Wall Street Journal, April 26, 2004.

Like spam, we must fight spyware on several fronts. Legislation, enforcement, customer education and technology solutions are all needed to combat this growing threat. We spoke here last April in support of H.R. 2929, the Safeguard Against Privacy Invasions (SPI) Act, which became the Securely Protect Yourself Against Cyber Trespass Act (SPY ACT) and which passed the House by a 399-1 margin last October. Similarly, we appear hear today in support of the efforts of Congresswoman Bono, her co-sponsors and this Committee to re-introduce this year's H.R. 29 the SPY ACT. Prohibiting the installation of software without a user's consent, requiring uninstall capability, establishing requirements for transmission pursuant to license agreements, and requiring notices for collection of personally identifiable information, intent to advertise and modification of user settings are all steps that will empower consumers and keep them in control of their computers and their online experience.

Various Forms of Spyware

Spyware comes in several different forms, each presenting unique threats:

Adware is advertising-supported software that displays pop-up advertisements whenever the program is running. Often the software is available online for free, and the advertisements create revenue for the company. Although it's seemingly harmless (aside from the intrusiveness and annoyance of pop-up ads), adware can install components onto your computer that track personal information (including your age, sex, location, buying preferences, or surfing habits) for marketing purposes.

Adware cookies are pieces of software that Web sites store on your hard drive when you visit a site. Some cookies exist just to save you time-for example, when you check a box for a Web site to remember your password on your computer. But some sites now deposit adware cookies, which store personal information (like your surfing habits, usernames and passwords, and areas of interest) and share the information with other Web sites. This sharing of information allows marketing firms to create a user profile based on your personal information and sell it to other firms.

System monitors can capture virtually everything you do on your computer, from keystrokes, emails, and chat room dialogue to which sites you visit and which programs you run. System monitors usually run in the background so that you don't know you're being watched. The information gathered by the system monitor is stored on your computer in an encrypted log file for later retrieval. Some programs can even email the log files to other locations. There has been a recent wave of system monitoring tools disguised as email attachments or free software products.

Trojan horses are malicious programs that appear as harmless or desirable applications. Trojan horses are designed to steal or encode computer data, and to destroy your system. Some Trojan horses, called RATs (Remote Administration Tools), give attackers unrestricted access to your computer whenever you're online. The attacker can perform activities like file transfers, adding or deleting files and programs, and controlling your mouse and keyboard. Trojan horses are distributed as email attachments, or they can be bundled with other software programs.

EarthLink’s Experience

As a leading Internet provider, EarthLink is on the front lines in combating spyware. EarthLink makes available to both its customers and the general public technology solutions to spyware such as EarthLink Spy Audit powered by Webroot (“Spy Audit”). Spy Audit is a free service that allows an online user to quickly examine his or her computer to detect spyware. A free download of Spy Audit is available at www.earthlink.net/spyaudit.   EarthLink members also have access to EarthLink Spyware Blocker, which disables all common forms of spyware including adware, system monitors, key loggers and Trojans. EarthLink Spyware Blocker is available free to EarthLink members as part of Total Access 2005, our Internet access software. See www.earthlink.net/home/software/spyblocker.

In addition to Spyware Blocker, Total Access 2005 includes a suite of protection tools such as spamBlocker, Pop-Up Blocker, Scam Blocker (which blocks phisher sites), Virus Blocker, and Parental Controls.

Over 3.2 million Spy Audit scans performed in the first 3 quarters of 2004 found over 83 million instances of spyware. This represents an average of 26 spyware programs per scanned PC. While most of these installations were relatively harmless adware and adware cookies, the scans revealed just over 1 million installations of more serious system monitors or Trojans.

Conclusion

Spyware is thus a growing problem that demands the attention of Congress, enforcement agencies, consumers and industry alike. Through the efforts of Congress to introduce legislation like the SPY ACT, enforcement actions by the FTC and other agencies, and through industry development of anti-spyware tools, we can all help protect consumers against a threat that is often unseen, but very much real.

Thank you for your time today.